



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/321,788	05/27/1999	ANTHONY J. NADALIN	AT9-99-081	7042

7590

05/12/2004

Law Office of Joseph R. Burwell
P.O. Box 28022
Austin, TX 78755-8022

EXAMINER

KIM, JUNG W

ART UNIT

PAPER NUMBER

2132

DATE MAILED: 05/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/321,788

Applicant(s)

NADALIN ET AL.

Examiner

Jung W Kim

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 17 March 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 11-28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 11-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 January 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: _____.

DETAILED ACTION

1. Claims 11-28 have been examined. The applicant in the amendment filed on January 26, 2004 has canceled claims 1-10 and amended claims 11-13 and 16-23. Claims 24-28 are new claims added by the applicant in the amendment filed on March 17, 2004.

Drawings

2. The drawings were received on January 30, 2004. These drawings are acceptable.

Specification

3. The substitute specification filed March 22, 2004 has been entered.

Claim Objections

4. Claim 24 is objected to because of the following informalities: since the claim is claiming a method comprising a series of steps, the preamble should indicate this listing as a series of steps. The following preamble is suggested: 'A method for enabling a program written in untrusted code to access in a trusted manner a resource supported on a computing device executing a native operating system, the method comprising the steps of:'.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 24 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: using the credential object by the program to access the resource within the native operating system by impersonating a security context of a native operating system user in accordance with the credential object (claim 24, last step; see specification, page 13, lines 19-24). This step is essential in the method to distinguish the step of '[accessing] in a trusted manner' as claimed in the preamble.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

8. Claims 11-13 and 17-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings Cryptography and Network Security 2nd Edition (hereinafter Stallings) in view of Bittinger et al. U.S. Patent No. 6,453,362 (hereinafter Bittinger), 'Moving Unix Applications to Windows NT' (hereinafter Praun), and Hunt TCP/IP

Network Administration (hereinafter Hunt). As per claim 17, Stallings discloses an authentication dialogue (see Stallings, pages 323-340, 'Kerberos') comprising the steps of:

- a. listening by a trusted login service for login requests (see Stallings, page 333, Figure 11.1, step 2, 'Authentication Server');
 - b. responsive to a login request for requesting a native operating system identifier by the trusted login service (see Stallings, page 333, Figure 11.1, step 2; page 331, Table 11.2, 'Authentication Service Exchange');
 - c. returning to the program the native operating system identifier (see Stallings, page 333, Figure 11.1, steps 2-3: response from AS to user; page 331, Table 11.2, 'Authentication Service Exchange', 'Message (2)');
 - d. in an authentication framework, using the native operating system identifier to create a credential object (see Stallings, page 333, Figure 11.1, step 4; page 332, Table 11.2, 'Ticket-Granting Service Exchange'); and
 - e. using the credential object to login to the server to enable the program to access the resource (see Stallings, page 333, Figure 11.1, steps 5-6; page 332, Table 11.2, 'Client/Server Authentication Exchange').
9. This authentication dialogue is disclosed as a service between a physical user and a trusted operating system and not between an untrusted code and a native operating system. However, 'users' of a secure OS generalize to include other types of relations such as an unprivileged client application gaining access to a secured server application. For example, Bittinger teaches a general login procedure whereby a client

application accesses a secured server application (see Bittinger, col. 5, lines 30-52; col. 7, lines 10-40; Figure 3, Reference Nos. 24 and 26). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Bittinger to the invention disclosed by Stallings. Motivation for such an implementation ensures that an untrusted client application is authenticated before gaining access to a trusted server application as taught by Bittinger.

10. Furthermore, Stallings is silent on the matter of establishing communication between the program and the trusted login service using named pipes. However, as taught by Praun, connections between two processes are typically made using named pipes when the receiving operating server process needs to assume the calling client's security context (see Praun, page 7, 1st paragraph). This impersonation enables the server to perform the required service at the lowest possible native user privilege but within the client's security context. Praun illustrates a simple scheme for a client process to access a service process using named pipes (see Praun, pages 19-43; 'Makefile', 'Readme.txt', 'Service.c' and 'Client.c', especially pages 27-28, 33-34 'ImpersonateNamedPipeClient()'). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Praun to the invention covered by Stallings. Motivation for such an implementation enables the native operating server to communicate with client applications and further provides means for server functions to run in the security context of a client application as taught by Praun.

11. Finally, Stallings is silent on the matter of the login request containing an identifier for a uniquely-named response pipe, wherein the uniquely-named response

Art Unit: 2132

pipe and the named pipe on which the trusted login service is listening for login requests are not identical. However, in the analogous art of TCP handshaking, Hunt teaches a means wherein a source generates a distinct pair (source port, destination port) and exchanges this pair to the destination: the destination using the source port value and destination port value received from the source as its destination port and source port respectively (see Hunt, page 49, Figure 2.7). In this scheme, the source transmits messages to the destination on the source port and listens on the destination port for a response by the destination. It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Hunt to the invention covered by Stallings since this type of configuration is a typical means for a system to dynamically connect with multiple clients as taught by Hunt (see Hunt, page 48, last paragraph-page 49, first paragraph). The aforementioned covers claim 17.

12. As per claim 18, Stallings covers a method as outlined above in the claim 17 rejection under 35 U.S.C. 103(a). In addition, the program executes in a virtual machine supported by the native operating system and the native operating system supports named-pipe servers (see Bittinger, col. 3, lines 1-3; col. 4, line 66-col. 5, line 7 as modified by Praun, page 19, Appendix A, 'Service Sample Source Code', 'Named pipe programing', last sentence).

13. As per claim 19, Stallings covers a method as outlined above in the claim 17 rejection under 35 U.S.C. 103(a). In addition, the program is written in an interpreted language (see Bittinger, col. 4, lines 66-67).

14. As per claims 11-13, they are method claims corresponding to claims 17-19 and they do not teach or define above the information claimed in claims 17-19. Therefore, claims 11-13 are rejected as being unpatentable over Stallings in view of Bittinger, Praun, and Hunt for the same reasons set forth in the rejections of claims 17-19.

15. As per claims 21-23, Stallings covers an application server as outlined above in the claim 17-19 rejections under 35 U.S.C. 103(a). In addition, the program written in untrusted code is one of a set of programs that are supported by a VM that is supported by a native operating system (see Stallings, page 324, 'Motivation' as modified by Bittinger, col. 5, lines 1-7), wherein each program written in untrusted code can run in an operating system thread while impersonating a different native operating system user (see Praun, page 7, 1st paragraph, API 'ImpersonateNamedPipeClient'). The aforementioned cover claims 21-23.

16. Claims 14, 16, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Bittinger, Praun, and Hunt, and further in view of Itoi et al. 'Pluggable Authentication Module for Windows NT' (hereinafter Itoi). As per claims 14 and 16, Stallings covers a method as outlined above in the claim 11 rejection

under 35 U.S.C. 103(a). Stallings is silent on the matter of the authentication framework being a pluggable authentication module (PAM). Itoi teaches a means for incorporating PAM into Windows NT as the authentication framework for the OS (Windows NT is the OS in the Praun example) (see Itoi, page 1, Sections 1 and 2; page 4, Figure 2.4). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Itoi to the invention covered by Bittinger. Motivation for such an implementation provides a generic and simple means to authenticate users as taught by Itoi.

17. As per claim 16, Stallings covers a method as outlined above in the claim 14 rejection under 35 U.S.C. 103(a). In addition, the authentication framework is compliant with an authentication service of a virtual machine (see Bittinger, col. 4, line 64-col. 5, line 40 as modified by Itoi, page 2, section 2.2 'Generic API for application programs').

18. As per claim 20, it is an apparatus claim corresponding to claims 16 and 17 and it does not teach or define above the information claimed in claims 16 and 17. Therefore, claim 20 is rejected as being unpatentable over Stallings in view of Bittinger, Praun, Hunt, and Itoi for the same reasons set forth in the rejections of claims 16 and 17.

19. Claim 15 is rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings in view of Bittinger, Praun, Hunt, and Itoi, and further in view of Win U.S. Patent No. 6,182,142 and Tang U.S. Patent No. 6,298,370. As per claim 15, Stallings covers a

method as outlined above in the claim 14 rejection under 35 U.S.C. 103(a). Itoi also describes API functions `pam_start()` and `pam_authenticate()` which corresponds to login interfaces, and `pam_end()` which corresponds to an abort interface (see Itoi, page 2, table 2.2). Although Itoi is silent on the matter of defining a commit and logout API, the activity of logging out a user is a consequence of logging in a user. Since logout is a standard feature of an authentication framework (see Win, col. 9, lines 31-38 for an example of a logout operation in an authentication framework) and commit operations are used to permanently enforce prior operations in programs dependent on strict sequential operation (see Tang, col. 131, lines 45-53 for a typical use of a commit operation), it would be obvious to one of ordinary skill in the art at the time the invention was made to include commit and logout APIs in the set of APIs found in the invention disclosed by Bittinger. The motivation for including the commit and logout APIs would be to establish a protocol of behavior for both the commit and logout tasks.

Allowable Subject Matter

20. Claims 24-28 would be allowable if rewritten or amended to overcome the rejection(s) under 35 U.S.C. 112, second paragraph, set forth in this Office action.

Response to Arguments

21. Applicant's arguments with respect to amended claims 11-23 have been considered but are moot in view of the new ground(s) of rejection.

Conclusion

22. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

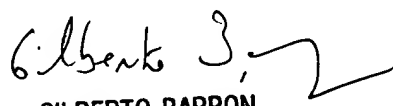
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Art Unit: 2132

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Jung W Kim
Examiner
Art Unit 2132

Jk
May 3, 2004


GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100